



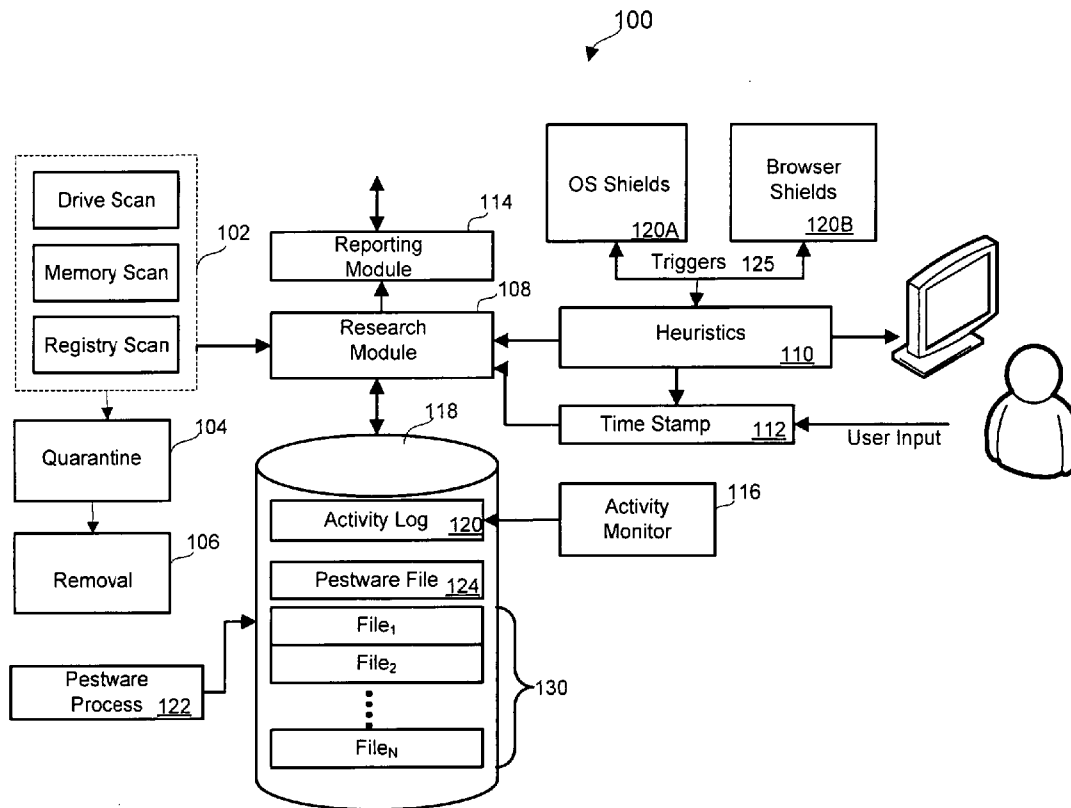
US 20070250818A1

(19) **United States**(12) **Patent Application Publication**
Boney(10) **Pub. No.: US 2007/0250818 A1**(43) **Pub. Date: Oct. 25, 2007**(54) **BACKWARDS RESEARCHING EXISTING
PESTWARE****Publication Classification**(76) Inventor: **Matthew L. Boney**, Longmont, CO
(US)(51) **Int. Cl.**
G06F 9/44 (2006.01)(52) **U.S. Cl.** 717/124

Correspondence Address:

COOLEY GODWARD KRONISH LLP
ATTN: PATENT GROUP
Suite 500
1200 - 19th Street, NW
WASHINGTON, DC 20036-2402 (US)(57) **ABSTRACT**

A system and method for researching a source of pestware on a computer is described. In one embodiment, the method includes identifying pestware on the computer, accessing recorded information on the computer relating to a history of the pestware and traversing at least a subset of the recorded information, wherein the traversing includes accessing data within the recorded information that provides a reference to an identity of a source of the pestware.

(21) Appl. No.: **11/408,215**(22) Filed: **Apr. 20, 2006**

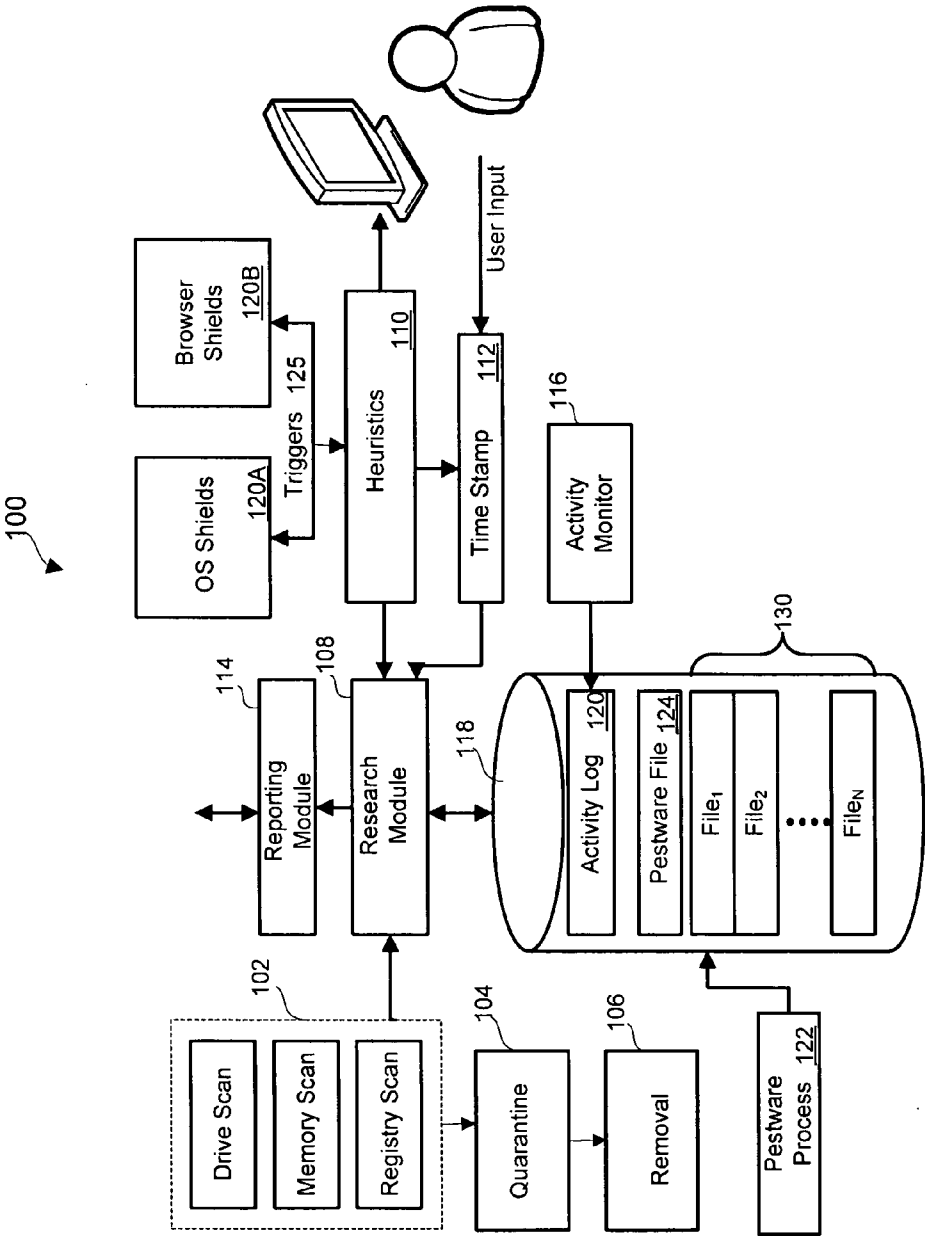


FIGURE 1

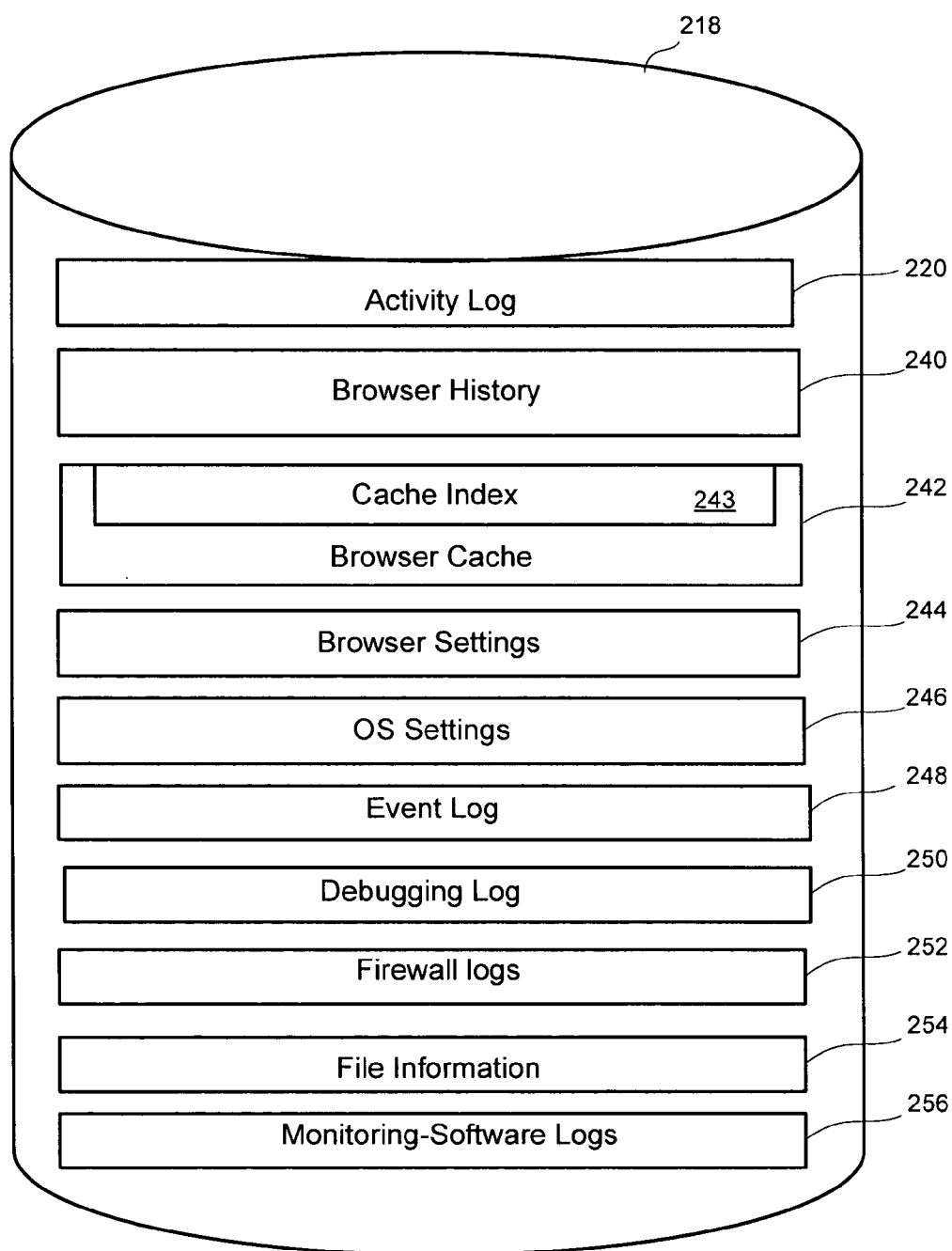


FIGURE 2

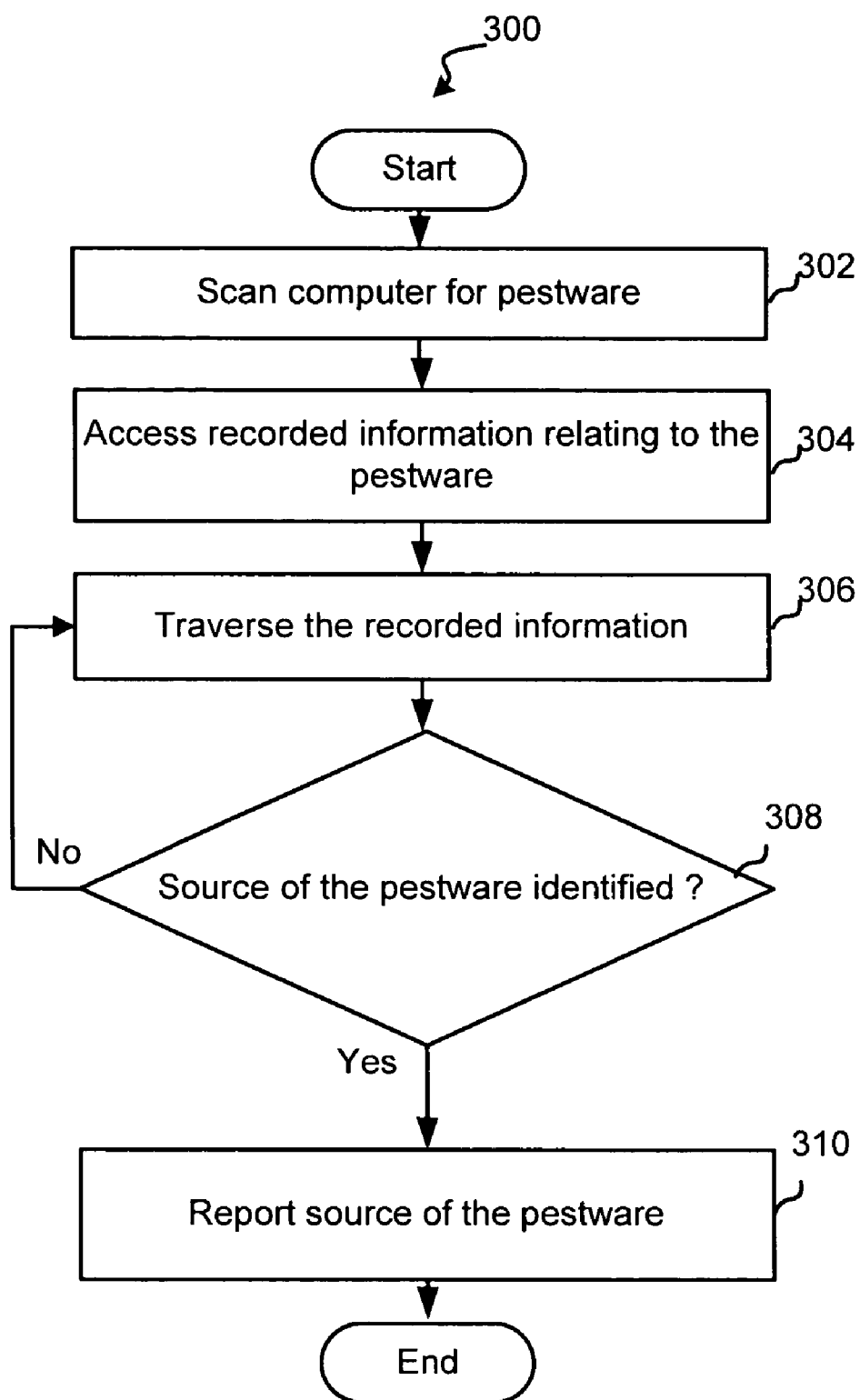


FIGURE 3

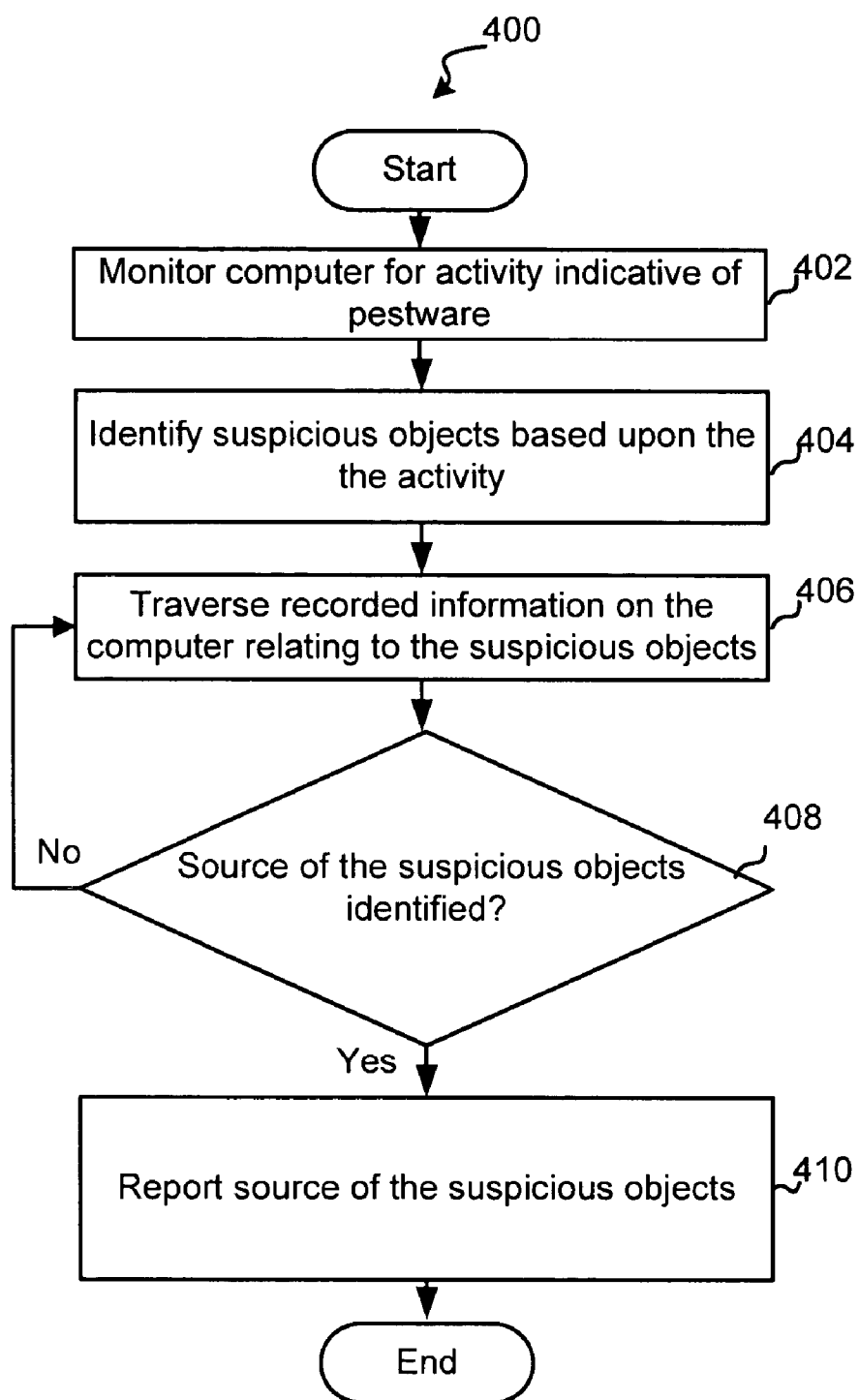


FIGURE 4

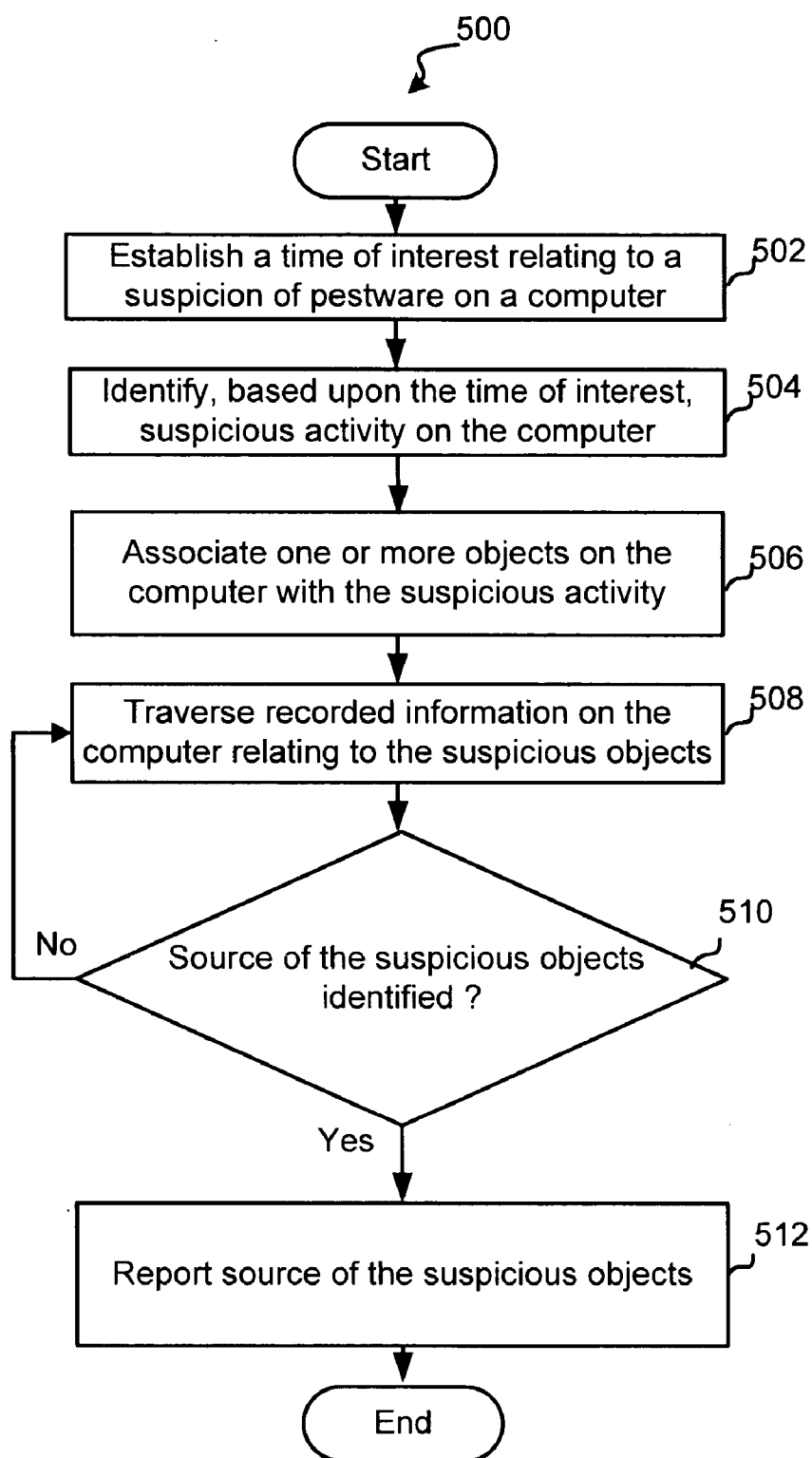


FIGURE 5

BACKWARDS RESEARCHING EXISTING PESTWARE

RELATED APPLICATIONS

[0001] The present application is related to commonly owned and assigned application Ser. No. 10/956,573, Attorney Docket No. WEBR-003/00US, entitled System and Method For Heuristic Analysis to Identify Pestware; application Ser. No. 10/956,574, Attorney Docket No. WEBR-005/00US, entitled System and Method for Pestware Detection and Removal; application Ser. No. 11/237,291, Attorney Docket No. WEBR-006/00US, entitled System and Method for Locating Malware and Generating Malware Definitions; application Ser. No. 11/257,609, Attorney Docket No. WEBR-015/00US, entitled System and Method for Kernel-Level Pestware Management; application Ser. No. 11/237,291, Attorney Docket No. WEBR-020/00US, entitled Client Side Exploit Tracking; application No. _____, Attorney Docket No. WEBR-044/00US, entitled Backwards researching Activity Indicative of Pestware, filed herewith; and application No. _____, Attorney Docket No. WEBR-045/00US, entitled Backward Researching Time Stamped Events to Find an Origin of Pestware, filed herewith, which are incorporated herein by reference.

COPYRIGHT

[0002] A portion of the disclosure of this patent document contains material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent disclosure, as it appears in the Patent and Trademark Office patent files or records, but otherwise reserves all copyright rights whatsoever.

FIELD OF THE INVENTION

[0003] The present invention relates to computer system management. In particular, but not by way of limitation, the present invention relates to systems and methods for detecting, controlling and/or removing pestware.

BACKGROUND OF THE INVENTION

[0004] Personal computers and business computers are continually attacked by trojans, spyware, and adware, collectively referred to as "malware," "spyware" or "pestware." These types of programs generally act to gather information about a person or organization—often without the person or organization's knowledge. Some pestware is highly malicious. Other pestware is non-malicious but may cause issues with privacy or system performance. And yet other pestware is actually beneficial or wanted by the user. Unless specified otherwise, "pestware" as used herein refers to any of these programs that collect information about a person or an organization.

[0005] Software is presently available to detect and remove pestware. But as it evolves, the software to detect and remove it must also evolve. Accordingly, current techniques and software for removing pestware are not always satisfactory and will most certainly not be satisfactory in the future. Additionally, because some pestware is actually valuable to a user, pestware-detection software should, in some cases, be able to handle differences between wanted and unwanted pestware.

[0006] Current pestware removal software uses definitions of known pestware to search for and remove files on a protected system. These definitions are often slow and cumbersome to create. Additionally, it is often difficult to initially locate the pestware in order to create the definitions. Accordingly, a system and method are needed to address the shortfalls of present technology and to provide other new and innovative features.

SUMMARY OF THE INVENTION

[0007] Exemplary embodiments of the present invention that are shown in the drawings are summarized below. These and other embodiments are more fully described in the Detailed Description section. It is to be understood, however, that there is no intention to limit the invention to the forms described in this Summary of the Invention or in the Detailed Description. One skilled in the art can recognize that there are numerous modifications, equivalents and alternative constructions that fall within the spirit and scope of the invention as expressed in the claims.

[0008] In one embodiment the invention may be characterized as a system and method for identifying a source of pestware on a computer. In one embodiment, the method includes identifying pestware on the computer, accessing recorded information on the computer relating to a history of the pestware and traversing at least a subset of the recorded information to an identity of a source of the pestware.

[0009] As previously stated, the above-described embodiments and implementations are for illustration purposes only. Numerous other embodiments, implementations, and details of the invention are easily recognized by those of skill in the art from the following descriptions and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] Various objects and advantages and a more complete understanding of the present invention are apparent and more readily appreciated by reference to the following Detailed Description and to the appended claims when taken in conjunction with the accompanying Drawings wherein:

[0011] FIG. 1 illustrates a block diagram of one implementation of the present invention;

[0012] FIG. 2 is a block diagram depicting an embodiment of the file storage device of FIG. 1;

[0013] FIG. 3 is a flowchart depicting a method according to an exemplary embodiment;

[0014] FIG. 4 is a flowchart depicting another method according to another embodiment;

[0015] FIG. 5 is a flowchart depicting yet another method according to yet another embodiment.

DETAILED DESCRIPTION

[0016] Referring now to the drawings, where like or similar elements are designated with identical reference numerals throughout the several views, and referring in particular to FIG. 1, it illustrates a block diagram of one implementation of the present invention. Shown is a protected computer 100 that includes a detection module 102, quarantine module 104, removal module 106, and shields

120. In addition, a research module **108** is shown coupled to a heuristics module **110**, a time stamp module **112** and a reporting module **114**.

[**0017**] Each of these modules can be implemented in software or hardware. And if implemented in software, the modules can be implemented in a single software package or in multiple software packages. In addition, one of ordinary skill in the art will recognize that the software can be designed to operate on any type of computer system including WINDOWS and Linux-based systems. Additionally, the software can be configured to operate on personal computers and/or servers. For convenience, embodiments of the present invention are generally described herein with relation to WINDOWS-based systems. Those of skill in the art can easily adapt these implementations for other types of operating systems or computer systems.

[**0018**] Also shown is a file storage device **118** that is coupled to the research module **108** and an activity monitor **116**. In this embodiment the file storage device includes an activity log **120**, a pestware file **124** and a collection of N files **130**. The file storage device **118** is described herein in several implementations as hard disk drive for convenience, but this is certainly not required, and one of ordinary skill in the art will recognize that other storage media may be utilized without departing from the scope of the present invention. In addition, one of ordinary skill in the art will recognize that the storage device **118**, which is depicted for convenience as a single storage device, may be realized by multiple (e.g., distributed) storage devices.

[**0019**] In the exemplary embodiment, the pestware file **124**, corresponds to (e.g., includes data relating to) a pestware process **122** operating in memory. The pestware process **122** is exemplary of pestware processes that are configured to make one or more unauthorized alterations to the computer **100**. For example, the pestware process **122** may make changes to either or both of the browser settings and/or operating system (OS) settings without approval and/or the knowledge of the user.

[**0020**] In accordance with several embodiments, the research module **108** is configured to receive an indication that either known pestware is residing on the computer or activities indicative of pestware have occurred or are occurring on the protected computer. In response, the research module **108** is configured to research the activity log **120** and/or the N files **130**, which include information (e.g., historical logs) relating to events on the computer **100**, to identify a source of the pestware **122**, **124** or pestware-related activities, which may be reported by the reporting module **114** to a centralized data store for subsequent pestware management purposes.

[**0021**] For example, the identities (e.g., I.P. address, URL, email client or program name) of sources (e.g., web sites, email or program) of the pestware may be collected in a centralized data store (not shown) and then subsequently reported to other users. In addition, the sources of the pestware or suspected pestware may be visited to further research how the pestware is being distributed from the URLs and/or to generate new definitions for pestware discovered at these sources.

[**0022**] As described further with reference to FIG. 2, the N files **130** include one or more files with information that

assist the research module **108** in tracing information in the N files **130** to an identity (e.g., URL) of the source of pestware **122**, **124** on the computer **100**. One or more of the N files **130** may be associated with an operating system of the protected computer and/or one or more applications of the protected computer, and may include information such as process IDs, registry entries, file names, cookies and URLs among other information that is used to trace from an identified pestware file, pestware process and/or pestware activity to an originating source (e.g., URL or IP address) of the infection. In one embodiment, one or more of the N files **130** is generated from an application that generates a log of data after examining the computer. An example of such an application is an application distributed under the name HijackThis.

[**0023**] In the exemplary embodiment depicted in FIG. 1, the research module **108** is configured to receive indications that pestware may be present on the computer from each of the detection engine **102**, the heuristics engine **110** and the time stamp module **112**, but this is certainly not required. In other embodiments, for example, the research module **108** may be configured to communicate only with the detection engine **102** or only with the heuristics engine. In yet other embodiments, the research module **108** may be configured to receive only a time stamp from the time stamp module **112**.

[**0024**] According to several embodiments, pestware-detection functions operating on the protected computer **100** are represented by the detection engine **102**, the quarantine engine **104**, the removal engine **106**, the shields **120** and the heuristic engine **110**. The basic functions of the detection engine **102** is to compare files, processes and registry entries on the protected computer against known pestware definitions and characteristics. When a match is found, in addition to quarantining and removing a pestware object, the detection engine **102** informs the research module **108** of the pestware. Details associated with several embodiments of sweep, quarantine, and removal engines are found in the above-identified application entitled System and Method for Pestware Detection and Removal.

[**0025**] Pestware and pestware activity can also be identified by the shields **120**, which generally run in the background on the computer system. In the exemplary embodiment depicted in FIG. 1, the shields **120** are divided into the operating system shields **120A** and the browser shields **120B**. The shields **120** are designed to watch for pestware and for typical pestware activity and includes two types of shields: behavior-monitoring shields and definition-based shields.

[**0026**] As an example, the shields **120** monitor the protected computer **100** for certain types of activities that generally correspond to pestware behavior. Particular examples of some of the types of activities that are monitored include a process spawning another process, an alteration to registry entries, communications with remote sites via the Internet, alterations to a start up folder, injection of a DLL into another process, and a change to the browser's home page and/or bookmarks. Some specific examples of shields are disclosed in the above-identified application entitled System and Method for Locating Malware and Generating Malware Definitions. In the exemplary embodiment, the shields **120** inform the heuristics engine **108** about

the activities and the heuristics engine **108** determines whether the research module **108** should be informed and/or whether the activity should be blocked.

[0027] As an example, the heuristics module **110** may compare the activities on the computer with weighted factors to make decisions relative to activities at the protected computer. Each of these factors may be, for example, associated with a particular activity and each factor may be weighted by the likelihood that the activity is associated with pestware. If the sum of the weighted factors that match the activity history exceed a threshold, then the activity is identified as pestware activity and the heuristics module **110** prompts the research module **108** to initiate research into the origin of the pestware initiating the activity. It should be recognized that this type of heuristics operation is merely one example, and that the heuristics module **110** may use other techniques to analyze activity on the computer. Additional information related to heuristics-based scanning is found in the above-identified applications entitled System and Method For Heuristic Analysis to Identify Pestware and Client Side Exploit Tracking.

[0028] In the exemplary embodiment depicted in FIG. 1, the time stamp module **112** is configured to send a time stamp to the research module **108** in response to a request from a user and/or in response to the heuristics module **108**. In some embodiments for example, the heuristics module **108** provides the user with information about suspect activity on the computer **100** so that the user has the option as to whether or not the research module **108** will attempt to identify the source of the activity.

[0029] In other embodiments, the heuristics module **110** prompts the time stamp module **112** to initiate the generation of a time stamp, without user intervention, in response to activity that is indicative of pestware activity. In one implementation, for example, the heuristics module **110** prompts the research module **108** to initiate tracing of the pestware activity to an origin of the pestware that is associated with the activity, and the heuristics module **110** also prompts the time stamp module **112** to send a time stamp **112** to the research module **108** so that the research module **108** is provided with a time reference as well as information about the pestware activities.

[0030] In yet other embodiments, the timestamp module **112** operates independently of the heuristics module **110**. For example, the timestamp module **112** may prompt the research module **108** to initiate a review of the activity log **120** and/or one or more of the N files in response to a user request.

[0031] The activity monitor **116** in several embodiments monitors activities on the computer and stores information about the activities in the activity log **120** so as to assist the research module **108** in identifying activities associated with pestware and the source of the pestware. In some embodiments, for example, the activity log **120** includes a list of processes that are running on the protected computer and the files that are associated with the processes. Although not depicted in FIG. 1, the shields **120** may utilize the activity monitor **116** to detect pestware-related events and intercept efforts by pestware to spawn new processes or alter aspects of the protected computer **100**.

[0032] In some variations, the activity monitor **116** may inject code into existing processes so that when a process

attempts to call a function of the computer's **100** operating system (not shown) the injected code can check the process to be started and raise a flag if the existing process is attempting to create a new pestware process or attempting to alter one or more settings (e.g., a registry setting) of the protected computer **100**.

[0033] In other embodiments, the activity monitor **116** is realized by a kernel-mode driver that may be loaded during a boot sequence for the protected computer or anytime later. In these embodiments, the activity monitor **116** is configured to log API calls in the activity log. In many variations for example, when a process (e.g., the pestware process) attempts to spawn a another pestware process or alter a registry entry, the API call utilized by the process is intercepted before it is carried out by an operating system of the protected computer. In this way, the attempt may be logged in the activity log **120** and the process may be analyzed to determine whether it is known to be a pestware-related process. Additional details of use of a kernel-level driver in connection with pestware management may be found in the above identified application entitled: System and Method for Kernel-Level Pestware Management.

[0034] It should be recognized that the block diagram in FIG. 1 depicts functional capabilities associated with several embodiments of the present invention. One of ordinary skill in the art will recognize that the functions described with reference to FIG. 1 may be realized by various implementations of software in connection with hardware or hardware alone. In these implementations several functions may be consolidated into a single module, for example, and as a consequence, may appear different from the block diagram in FIG. 1 without departing from the scope of the present invention.

[0035] Referring next to FIG. 2, shown are exemplary resources, also referred to herein as historical logs, that are available to the research module **108** in accordance with one embodiment of the present invention. In general, these resources are logs of historical events that occurred on the computer, and each of the logs includes information that may be used to reference other information when, for example, activities, processes and files are traced so as to determine an origin of the pestware or suspected pestware. As shown, a file storage device **218** in this embodiment includes an activity log **220**, which may be generated by an activity monitor (e.g., the activity monitor **116**) and may include information about processes running on the computer **100** and files corresponding to the processes. In variations, the activity log **220** includes a history of API calls and respective times made by processes running on the protected computer, but this is certainly not required.

[0036] In addition, the file storage device **218** includes a browser history **240**, browser cache **242**, browser settings **244**, OS settings **246**, an event log **248**, a debugging log **250**, a firewall log **252**, file information **254** and monitoring software logs **256**. One or more of these exemplary files **240-256** may be implemented for one or more of the N files **130** described with reference to FIG. 1.

[0037] The browser history **240** in this embodiment includes a listing of web sites and respective times that the web sites were visited by the user. The browser cache **242** in this embodiment includes files, cookies, and other objects cached in connection with use of a browser of the protected

computer (e.g., Internet Explorer or Mozilla (not shown)). As depicted, the browser cache **242** includes a cache index **243** that includes a listing, which associates the content of the browser cache **242** with URLs and time stamps. As discussed further herein, the cache index **243** provides an efficient means for identifying the times objects were retrieved and the URLs that the objects were retrieved from.

[0038] The browser settings **244** include information about settings associated with a browser and may include a home page setting and list of user favorites. The browser settings **244** are monitored by the shields **120** for changes. Those settings also contain URLs that may be referenced in time stamped logs, firewall logs, browser histories, etc.

[0039] The operating system (OS) settings **246** may include registry entries, a start up folder and other information utilized by an operating system of the protected computer. As discussed further herein, data included in the OS settings **246** may include time stamps, which indicate when changes were made to the settings.

[0040] The event log **248** in this embodiment includes a log of events that is maintained by an operating system of the protected computer **100**. For example, the event log **248** may include event information including errors, user log-in history, a listing of processes that have been launched (and the users that launched the processes), path information, information about which process (and which users) accessed a secure area and other information relating to operations of the computer **100**.

[0041] Also shown in FIG. 2 is a debugging log **250** that includes application errors, which point to a process and the address where the error occurred. Some techniques employed by pestware forcibly shut down applications, or cause applications to crash when their memory space is injected with pestware code. The infected applications like "explorer.exe" will crash, or some times restart spontaneously. These events/occurrences show up in debugging logs. These are time stamped events, that also reference files on the system.

[0042] The firewall log **252** in this embodiment is a collection of information relating to network-related events on the protected computer. The firewall log **252**, may for example, include time stamps of network activities on the protected computer, which may be utilized by the research module **108** to locate pestware or indicia of pestware.

[0043] Also shown in the data storage device **218** is a collection of file information **254**, also known as the file system, which includes a database that the operating system uses to locate and store information about files. For example, the file information **254** may include the date and time a file is created, a date and time the file was last modified, the date and time the files was last accessed and the size of the file.

[0044] The monitoring-software logs **256** includes information collected from one or more pieces of monitoring software that are configured to monitor activity on the computer. As an example, the monitoring logs **256** may be generated from a filter driver, a module interfacing with a layer service provider and/or browser helper objects. It should be recognized that the logs **220, 240-256** depicted in FIG. 2 are merely exemplary and these logs are by no means representative all the potential logs that may be accessed to research origins of pestware and/or suspected-pestware.

[0045] Referring next to FIG. 3, shown is a flowchart depicting a method in accordance with one embodiment. Although reference will be made to FIGS. 1 and 2 for exemplary purposes, it should be recognized that the method described with reference to FIG. 3 is certainly not limited to the specific embodiments described with reference to FIGS. 1 and 2. As shown, in this embodiment a scan of a computer (e.g., the computer **100**) for pestware is initially carried out (Block **302**). In several embodiments for example, the detection engine **102** scans the file storage device **118**, the operating system registry and executable memory of the protected computer for indicia of pestware (e.g., processes or files matching pestware definitions and/or alterations to a registry entry that are consistent with pestware).

[0046] As shown in FIG. 3, if pestware indicia is found, then recorded information (e.g., the activity log **120** and/or the N files **130**) that may include traces of the pestware is accessed (Block **304**), and traversed to search for information leading to the identification of the source of the pestware (Block **306**). In some instances, the origin of the pestware may be identified by simply referencing one piece of data that is stored in connection with the identification of the pestware source. In other instances, however, it may be necessary to access several pieces of referential data, which may be located in one or more of the files **220-256** before arriving at the identity of the source of the pestware.

[0047] As an example, if a pestware file is found on the file storage device **118**, then the cache index **243** of the browser cache **242** may be searched to identify the name of the file, and if the originating URL is stored in connection with the file, the URL is identified as the source of the file. As another example, if a pestware process is identified, a search of the activity log **220** may lead to the identity of a second process that spawned the pestware process, and additional searching of the activity log **220** using the name of the second process may lead to the identification of a pestware file associated with the second process. In turn, a search of the cache index **243** for the name of the pestware file may lead to the URL from which the pestware file was downloaded.

[0048] As shown in FIG. 3, if the source of the pestware is identified (Block **308**), then the source of the pestware is reported (Block **310**). In some embodiments, it is contemplated that several other computers configured in accordance with the protected computer **100** depicted in FIG. 1 may also report sources of pestware to a centralized location where the URLs may be added to a list of "bad URLs." In addition, the identified URLs may be actively searched to learn more about the pestware generated at the sites, which may help generate definitions for the pestware and may provide information about how pestware infections occur.

[0049] Referring next to FIG. 4, shown is a flowchart depicting a method in accordance with another embodiment of the present invention. Again, reference will be made to FIGS. 1 and 2 for exemplary purposes, but it should be recognized that the method described with reference to FIG. 4 is certainly not limited to the specific embodiments described with reference to FIGS. 1 and 2. As shown, in this embodiment activity on a computer is monitored for indicia of pestware (Block **402**), and if potential pestware-related activity is detected, recorded information related to the activity is searched to identify one or more suspicious objects (e.g., files and/or processes) that are related to the

activity (Block 404). In some embodiments, the shields 120 (described with reference to FIG. 1) may monitor the protected computer 100 for activities, and if the activity is identified as potential pestware activity (e.g., by the heuristics module 110), then the research module 108 searches the activity log 120 and/or one or more of the N files for information relating to the pestware-related activity.

[0050] As shown in FIG. 4, recorded information (e.g., one or more of the N files) is then traversed to trace through information related to the suspicious objects that leads to an origin of the suspicious objects (Block 406). In one embodiment for example, the suspicious activity leads to a search for suspicious processes and/or files related to the activity (e.g., using the activity log 120), which then leads to a search of one or more of the N files 130 (e.g., the cache index 243) for an indication of the source of the suspicious process and/or files.

[0051] As depicted in FIG. 4, if the source of the suspicious object(s) is identified (Block 408), then the source of the suspicious object(s) is then reported (e.g., to a pestware research entity). In this way, the suspicious objects and the web sites originating the suspicious objects may be further researched to establish the extent to which they may be a threat.

[0052] As an example of pestware-related activity that may trigger the search for a source of the activity, if a series of particular API calls is made in a pattern known to be associated with pestware, the process(es) making the calls may be identified using, for example, the activity log 120. In turn, the activity log 120 may be used to identify the file(s) associated with the process(es), and the cache index 243 may be utilized to search for a source of the file(s). It should be recognized that this is merely one example of the type of activity that may trigger backwards researching of logs on a computer, and that patterns in process creation, downloaded files, changes to an operating system registry and browser settings, for example, may trigger a search of the computer's logs.

[0053] Referring next to FIG. 5, shown is a flowchart depicting yet another method in accordance with another embodiment of the present invention. While referring to FIG. 5, simultaneous reference will be made to FIGS. 1 and 2 for exemplary purposes, but it should be recognized that the method described with reference to FIG. 5 is certainly not limited to the specific embodiments described with reference to FIGS. 1 and 2.

[0054] As shown, in this embodiment a time of interest is initially established based upon a suspicion that pestware has infected a computer (Block 502). In some embodiments, for example, a user may establish the time of interest based upon events the user observed (e.g., pop-ups or a system crash). In one embodiment, as discussed with reference to FIG. 1, in response to a user request, the time stamp module 112 may issue a time stamp and initiate research that is related to activity occurring at or around the time of the time stamp. In variations, the user is provided with an alert in response to the heuristics module 110 identifying an activity that is suspicious and the user is given an option to initiate research at or around the time of interest.

[0055] In other embodiments, the time stamp module 112 automatically generates a time stamp in response to a report of suspicious activity (e.g., from the shields 120 or heuristics module 110).

[0056] As shown in FIG. 5, once a time of interest is established, suspicious activity is identified on the computer based upon the time of interest (Block 504). The time of interest may be established, for example, to include a time period before the time stamp is issued so that a search for suspicious activity is limited to a particular time period. In some embodiments, the activity log 130 and/or one or more of the N files 130 are accessed and analyzed to determine whether any activity during the time of interest is suspicious (e.g., the activity indicates in some way that it may be associated with pestware). As an example, if any logged information (e.g., in the activity log 130 and/or one or more of the N files 130) indicates that during the time of interest that, for example, access to the registry was carried out in connection with a downloaded file or the launch of a process, the activities may be identified as being suspect and further research relative to the process and the file may be carried out.

[0057] Beneficially, many of the logs accessed include time-stamped information, which enables an activity that occurred during the time of interest to be readily identified and analyzed either alone or in connection with other activities occurring during the time of interest. As an example, the activity log 220, the browser history 240, browser cache 242, operating system settings 246, the event log 248, the debugging log 250 the firewall log 252, the file information 254 and the monitoring software logs 256 include time stamped information that provides insight into the activities that occurred on the computer during the time of interest.

[0058] As depicted in FIG. 5, once one or more activities are identified as being suspicious (Block 504), one or more objects (e.g., processes or files) on the computer are associated with the suspicious activity (Block 506). For example, the research module 108 may search the activity log 120 and/or one or more of the N files for information that associates the suspicious activity to one or more processes and the processes may be related to one or more files.

[0059] As shown in FIG. 5, recorded information on the computer is then traversed in order to trace to an origin of one or more of the objects (Block 508). For example, a search of one or more of the N files 130 (e.g., the cache index 243) may be carried out to identify the source of a suspicious process and/or files. Once the source of the suspicious object(s) is identified (Block 510), the source is then reported (e.g., to a remote research entity) (Block 512).

[0060] It should be recognized that the methods described with reference to FIGS. 3, 4 and 5 are merely exemplary and are certainly not the only modes of operation that are contemplated. As an example, the establishment of a time of interest, as discussed with reference to FIG. 5, may be useful in the method described with reference to FIGS. 3 and 4 for identifying information that leads to the source of the pestware or pestware-related activities. Moreover, it is contemplated that aspects from all three of the methods described with reference to FIGS. 3, 4 and 5 may be combined.

[0061] In conclusion, the present invention provides, among other things, a system and method for identifying a source of pestware or suspected pestware on a computer. Those skilled in the art can readily recognize that numerous variations and substitutions may be made in the invention,

its use and its configuration to achieve substantially the same results as achieved by the embodiments described herein. Accordingly, there is no intention to limit the invention to the disclosed exemplary forms. Many variations, modifications and alternative constructions fall within the scope and spirit of the disclosed invention as expressed in the claims.

What is claimed is:

1. A method for identifying an origin of pestware residing on a computer comprising:

identifying pestware on the computer;

accessing recorded information on the computer relating to a history of the pestware; and

traversing at least a subset of the recorded information, wherein the traversing includes accessing data within the recorded information that provides a reference to an identity of a source of the pestware.

2. The method of claim 1, including:

reporting the source of the pestware to a pestware research entity so as to enable the pestware research entity to place the identity of the source of the pestware in a repository that includes identities of other sources of pestware.

3. The method of claim 1, wherein the identifying includes scanning processes and files of the computer.

4. The method of claim 1, wherein the identifying includes identifying a pestware process; wherein the traversing includes:

accessing recorded information that associates the pestware file with the source of the pestware so as to identify the source of the pestware.

5. The method of claim 1, including:

monitoring a pestware process on the computer;

recording in an activity log, an attempt by the pestware process to launch another process from a stored file;

wherein the traversing includes identifying a reference to the stored file in the recorded information and identifying a reference to an identity of the source of the file using the reference to the stored file.

6. The method of claim 5, wherein the monitoring includes monitoring the process with a kernel-mode driver.

7. The method of claim 1, wherein the source is identified by an identifier selected from the group consisting of an I.P. address, a URL, an email client and a program name.

8. The method of claim 1, wherein the accessing includes accessing the recorded information from a file stored on the computer that is selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs.

9. A system for identifying a source of pestware on a computer including:

a detection portion configured to detect pestware on the computer; and

a research portion configured to access recorded information on the computer relating to a history of the pestware and to access data within the recorded information that provides a reference to an identity of a source of the pestware;

a reporting portion configured to report the source of the pestware to a pestware research entity.

10. The system of claim 9, wherein the detection portion includes a drive scan portion configured to detect pestware on a file storage device of the computer, a memory scan portion configured to detect pestware residing in an executable memory of the computer and a registry scan portion configured to scan a registry of an operating system of the computer for indicia of pestware.

11. The system of claim 10, including:

an activity monitor configured to monitor API calls and to store a history of at least a portion of the API calls in an activity log.

12. The system of claim 11, wherein the activity monitor is configured to store a history of API calls to create processes along with information about files associated with the processes in the activity log, and wherein the research portion is configured to access the activity log in order to identify a file associated with a pestware process that was identified as pestware by the scanning portion as pestware.

13. The system of claim 11, wherein the activity monitor includes a kernel-mode driver adapted to intercept the API calls.

14. The system of claim 9, wherein the source is identified by an identifier selected from the group consisting of an I.P. address, a URL, an email client and a program name.

15. The system of claim 9, wherein the recorded information is recorded in a file selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs.

16. A computer-readable medium encoded with processor-executable instructions for identifying an origin of pestware residing on a computer, the instructions including instructions for:

identifying pestware on the computer;

accessing recorded information on the computer relating to a history of the pestware; and

traversing at least a subset of the recorded information, wherein the traversing includes accessing data within the recorded information that provides a reference to an identity of a source of the pestware.

17. The computer-readable medium of claim 16, including instructions for:

reporting the source of the pestware to a pestware research entity so as to enable the pestware research entity to place the identity of the source of the pestware in a repository that includes identities of other sources of pestware.

18. The computer-readable medium of claim 16, wherein the instructions for identifying includes instructions for scanning processes and files of the computer.

19. The computer-readable medium of claim 16, wherein the instructions for identifying includes instructions for identifying a pestware process and wherein the instructions for traversing include instructions for:

accessing recorded information that associates the pestware process with a pestware file so as to identify the pestware file; and

accessing recorded information that associates the pestware file with the source of the pestware so as to identify the source of the pestware.

20. The computer-readable medium of claim 16, including instructions for:

monitoring a pestware process on the computer;

recording in an activity log, an attempt by the pestware process to launch another process from a stored file;

wherein the instructions for traversing include instructions for identifying a reference to the stored file in the recorded information and identifying a reference to an identity of the source of the file using the reference to the stored file.

21. The computer-readable medium of claim 20, wherein the instructions for monitoring include instructions for monitoring the process with a kernel-mode driver.

22. The computer-readable medium of claim 16, wherein the source is identified by an identifier selected from the group consisting of an I.P. address, a URL, an email client and a program name.

23. The computer-readable medium of claim 16, wherein the instructions for accessing include instructions for accessing the recorded information from a file stored on the computer that is selected from the group consisting of: an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs.

* * * * *